APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,949	04/02/2004	Chen-Huang Fan	ACMP0048USA	4656

27765   7590   03/25/2008
NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
03/25/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

winstonhsu.uspto@gmail.com
Patent.admin.uspto.Rcv@naipo.com
mis.ap.uspto@naipo.com.tw

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 December 2007*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Applicant's arguments filed December 28, 2007, have been fully considered but they are not persuasive.

2.   Claims 1-24 are pending and have been examined.

Response to Amendment

3.   Regarding the argument that the patent does not use inerasable memory, Examiner respectfully submits that the claim language used in the patent makes it clear that the generating module dies not store information generated, therefore anticipating using inerasable memory in the instant application. **Applicant's arguments are not persuasive.**

4.   The arguments presented above with respect to the double patenting rejections, pertain to the 35 U.S.C. 102(f) rejection. **Applicant's arguments are not persuasive.**

5.   Regarding the argument that Kirsch does not teaches unreadable information that affords the decryption of data, Examiner respectfully submits that the decrypting function is stored in read only memory as correctly pointed out by applicant. Furthermore, the function and the key data stored in user module are inerasable/read-only, etc, as they only receive writing instruction internally, not from external information or commands, in other words, from a user's perspective the information is inerasable. **Applicant's arguments are not persuasive.**

6.   The invention describes the inerasable key not only as memory, but a key stored in a protective manner (see par. 10). Examiner has given the claims the broadest reasonable interpretation consistent with the specification.

7.   Even assuming arguendo Examiner is incorrect, **using** read-only memory to store information that is not intended to be modified by a user/program was conventional and well known. Therefore, Kirsch provides at the very least, the architecture to implement the claimed invention, since the only modification the claimed invention allegedly makes is to replace one memory type for another. **Applicant's arguments are not persuasive.**

Information Disclosure Statement

8.   It is noted that no Information Disclosure Statement has been filed on this application.

Double Patenting

9.   Claims 1-24 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-22 of US Patent 7,177,425.

10.   Although the conflicting claims are not identical, they are not patentably distinct from each other because

-       "determining whether a communication device is permitted to access communication service in a communication network, the communication device comprising: a data memory capable of storing ciphertext access information; and an inerasable memory capable of storing a deciphering key in a non-volatile way; the method comprising: reading the deciphering key in the inerasable memory and the ciphertext access information in the data memory; and deciphering the ciphertext access information to plaintext access information according to the deciphering key by using a predetermined cryptography algorithm, and determining whether the communication device is

permitted to access communication service in the communication network accordingly"

(claim 1, instant application) is analogous to

- "A device, used in a communication apparatus, for securing an information associated

with a subscriber, said communication apparatus comprising a cipher-key generating

module for generating a cipher key, said device comprising: a storage module, which

the information associated with the subscriber, is stored in; a cipher-key acquiring

module for transmitting an input to the cipher-key generating module, and then

receiving the cipher key generated by the cipher-key generating module in response to

the input; an encrypting module for retrieving the cipher key through the cipher-key

acquiring module, retrieving the information associated the subscriber from the storage

module, and encrypting the information associated with the subscriber using the cipher

key to generate an encrypted information, wherein after generated, the encrypted

information is stored in the storage module and replaces the information associated with

the subscriber stored in the storage module; and a decrypting module for retrieving the

cipher key through the cipher-key acquiring module, retrieving the encrypted information

from the storage module, and decrypting the encrypted information using the cipher key

to recover the information associated with the subscriber when the information

associated with the subscriber needs to be used, and wherein when the decrypting

module retrieves the cipher key through the cipher-key acquiring module, the cipher-key

acquiring module transmits the input once more to the cipher-key generating module,

and then receives the cipher key generated once more by the cipher-key generating

module in response to the input" (claim 1, Patent).

11.   This is a provisional obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

12.   Claims 1-22 of US Patent 7,177,425 contain every element of claims 1-24 of the instant application and thus anticipate the claims of the instant application. Claims 1-24 of the instant application therefore are not patently distinct from the patent claims and as such are unpatentable for obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

13.   "A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species with that genus). "ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

14.   "Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is "anticipated" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4. This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic claim. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); Schneller, 397 F.2d at 354. Accordingly,

absent a terminal disclaimer, claims 12 and 13 were properly rejected under the

doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d

2010 (12/3/1993).

Claim Rejections - 35 USC § 102

15.   The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

16.   **Claims 1-24 are rejected under 35 U.S.C. 102(f) because the applicant did**

not invent the claimed subject matter.

See Double Patenting rejection above and the Patent's inventors conflict.

17.   **Claims 1-24 are rejected under 35 U.S.C. 102(e) as being anticipated by**

Kirsch et al. (US Patent Application Publication 2005/0120225, hereinafter Kirsch).

Regarding claims 1 and12, Kirsch teaches

- a method for determining whether a communication device is permitted

    to access communication service in a communication network, the

    communication device comprising **(abstract, user and configuration**

    data):

- a data memory capable of storing ciphertext access information **(pars. 8-**

    11, user data in encrypted form); and

- an inerasable memory capable of storing a deciphering key in a non-

    volatile way **(pars. 34-36, non-volatile memory stores keys and**

    cryptographic functions);

- the method comprising: reading the deciphering key in the inerasable memory and the ciphertext access information in the data memory **(pars. 44-47, execute function using key)**; and

- deciphering the ciphertext access information to plaintext access information according to the deciphering key by using a predetermined cryptography algorithm **(pars. 45-50, using private key)**, and

- determining whether the communication device is permitted to access communication service in the communication network accordingly **(pars. 26-28, 35-42, permitting access upon validation)**.

Regarding claim 20, Kirsch teaches

- a method applied in a communication network, wherein the communication network comprises a plurality of communication devices and each communication device comprises an inerasable memory and a data memory **(abstract, user and configuration data)**;

- the method being capable of determining whether each communication device is permitted to access communication service of the communication network **(pars. 26-28, 35-42, permitting access upon validation)**;

- the method comprising: providing a plurality of different enciphering keys and a plurality of deciphering keys according to a cryptography algorithm **(pars. 44-47, execute function using key)**,

- wherein each enciphering key corresponds to each deciphering key **(pars. 47-49, asymmetrical RSA)**;

- providing different corresponding enciphering keys to different communication devices **(pars. 47-49, asymmetrical RSA)**;

- enciphering access information corresponding to each communication device to ciphertext access information by the cryptography algorithm according to the enciphering key corresponding to the communication device **(pars. 8-11, user data in encrypted form)**;

- storing deciphering keys corresponding to the enciphering keys corresponding to each of the communication devices in the inerasable memory **(pars. 34-36, non-volatile memory stores keys and cryptographic functions)**;

- storing ciphertext access information of each communication device in the data memory of the communication device **(pars. 8-11, user data in encrypted form)**; and

- when determining whether a communication device is permitted to access the communication service **(pars. 26-28, 35-42, permitting access upon validation)**,

- deciphering the ciphertext access information in the data memory by the cryptography algorithm according to the enciphering key stored in the inerasable memory **(pars. 45-50, using private key)**, and

- determining whether the communication device is permitted to access the communication service according to the deciphered ciphertext access information **(pars. 26-28, 35-42, permitting access upon validation)**.

Regarding claims 2, 13, and 22, Kirsch teaches wherein the cryptography

algorithm is an asymmetric encryption-and-decryption algorithm / such that an

enciphering key is not equal to the corresponding deciphering key, and when a plaintext

is enciphered into a ciphertext according to the enciphering key by the cryptography

algorithm, the cryptography algorithm cannot decipher the ciphertext into the original

plaintext according to the enciphering key **(pars. 47-49, asymmetrical RSA)**.

Regarding claim 3, Kirsch teaches wherein the data memory is a non-volatile

memory **(pars. 32-33, ROM)**.

Regarding claims 4 and 14, Kirsch teaches

- enciphering access information corresponding to the communication device

    into the ciphertext access information by the cryptography algorithm

    according to an enciphering key **(pars. 8-11, user data in encrypted form)**,

- wherein the enciphering key corresponds to the deciphering key; and

    recording the ciphertext access information in the data memory **(pars. 47-49,**

    asymmetrical RSA).

Regarding claims 5 and 15, Kirsch teaches generating the enciphering key and

the corresponding deciphering key according to the cryptography algorithm before

generating the ciphertext access information according to the enciphering key **(pars.**

50-51).

Regarding claims 6, 16, and 23, Kirsch teaches wherein the communication

network comprises a service provider capable of providing communication service to the

communication device; there being a database in the service provider for recording the

enciphering key and the access information corresponding to the communication device

(pars. 51-52, storing at ASP).

Regarding claim 7, Kirsch teaches wherein when generating the ciphertext

access information according to the enciphering key, the service provider enciphers the

access information corresponding to the communication device to generate the

ciphertext access information according to the enciphering key stored in the database

(pars. 51-52, storing at ASP).

Regarding claim 8, Kirsch teaches wherein when recording the ciphertext

access information in the data memory, transmitting the ciphertext access information

from the service provider to the communication device via the communication network,

and recording the ciphertext access information in the data memory with the

communication device **(pars. 50-53, storing at ASP and synchronizing)**.

Regarding claims 9 and 21, Kirsch teaches wherein the enciphering key is

different from the deciphering key / wherein the deciphering keys corresponding to

different enciphering keys are different **(pars. 47-49, asymmetrical RSA)**.

Regarding claims 10 and 17, Kirsch teaches wherein when determining

whether the communication device is permitted to access communication service of the

communication network according to the plaintext access information, determining

whether the plaintext access information conforms to predetermined access information;

the communication device being determined permitted to access the communication

service of the communication network if the plaintext access information conforms to the

predetermined access information **(pars. 26-28, 35-42, permitting access upon**

validation).

Regarding claims 11 and 18, Kirsch teaches

- in which the communication device further comprises a subscriber

  identification module card (SIM card) capable of recording a subscriber

  identification number **(pars 26-28, SIM)**,

- and a predetermined identification number is recorded in the plaintext access

  information **(pars 26-28, identity module)**,

- wherein when determining whether the communication device is permitted to

  access communication service in the communication network according to the

  plaintext access information **(pars. 26-28, 35-42, permitting access upon**

  validation),

- determining whether the subscriber identification code conforms to the

  predetermined identification code; the communication device being permitted

  to access the communication service if the predetermined identification code

  and the subscriber identification code correspond to each other, and the

  communication device being not permitted to access the communication

  service and having access to the communication network stopped if the

  predetermined identification code and the subscriber identification code do

  not correspond to each other **(pars. 26-28, 35-42, permitting access upon**

  validation).

Regarding claims 19 and 24, Kirsch teaches in which the communication device is a cell phone, and the communication network is a wireless communication network **(pars. 24-28, mobile telephone, par. 25, wireless device, service provider)**.

Conclusion

18.   **Examiner's Note:** Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

19.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

20.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

21.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

22.   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136